Wireless Personal Communications (2020) 112:193–224
https://doi.org/10.1007/s11277-019-07022-5

A Smart Approach for Intrusion Detection and Prevention System in Mobile Ad Hoc Networks Against Security Attacks

M. Islabudeen[1] · M. K. Kavitha Devi[2]

Published online: 2 January 2020

Abstract
Design of intrusion detection and prevention scheme for improving MANET security, with considered energy efficiency, detection rate, delay, and false positive rate are major research issues. Most of the existing solutions have suffered to obtain accurate detection rate in minimal time execution and energy consumption. In this work we proposed a Smart approach for intrusion detection and prevention system (SA-IDPS) to mitigate attacks in MANET by machine learning methods. Initially, mobile users are registered in Trusted Authority using One Way Hash Chain Function. Each mobile user submits their following information to verify authentication: finger vein biometric, user id, and latitude and longitude. Intrusion detection is executed using four entities: Packet Analyzer, Preprocessing Unit, Feature Extraction Unit and Classification Unit. In packet analyzer, we verify whether any attack pattern is found or not. It is implemented using Type 2 Fuzzy Controller which considers information from packet header. In preprocessing unit, logarithmic normalization and encoding schemes are considered, which is time series and suitable for any application. In feature extraction unit, Mutual Information is used where we extracts optimum set of features for packets classification. In classification unit, Bootstrapped Optimistic Algorithm for Tree Construction with Artificial Neural Network is used for packets classification, which classifies packets five classes: DoS, Probe, U2R, R2L, and Anomaly, and then Association Rule Tree are used to classify whether the attack is Frequent or Rare. In this case, historical table is used for packets classification. Finally, experiments are conducted and tested for evaluating the performance of proposed SA-IDPS scheme in terms of Detection Rate (%), False Positive Rate (%), Detection Delay (s), and Energy Consumption (J).

Keywords Mobile ad hoc network · Intrusion detection and prevention · Type 2 fuzzy controller · BOAT with ART · Artificial neural networks

✉ M. Islabudeen
islabudeen@gmail.com

M. K. Kavitha Devi
mkkdit@tce.edu

[1] Department of CSE, Syed Ammal Engineering College, Ramanathapuram, India

[2] Department of CSE, Thiagarajar College of Engineering, Madurai, India

1 Introduction

MANET is a type of self-configuring wireless network consists of mobile nodes connected via wireless links. Each mobile node will act as router. Mobile nodes are vulnerable due to its significant features such as dynamic topology, constrained capability, distributed cooperation, and open medium. Intrusion Detection and Prevention System (IDPS) is presented recently to detect and mitigate the security attacks in MANET [1, 2]. In conventional IDPS, individual node is required to run in the IDS agent to monitor intrusions, but this case does not suitable to detect attacks [3]. Intruders in MANET are classified as three classes: Masquerader, Misfeasor, and Clandestine User. Masquerader is an outsider who intend to access legitimate mobile nodes in unauthorized manner. Misfeasor is an insider, who misuse legitimate nodes privilege and clandestine user is either insider, or outsider, who intend to hold supervisory control on MANET [4–6]. IDPS is an important security element nowadays for any wireless networks. Intrusion detection refers to detection of malicious activities such as attacks, penetrations, break-ins, and so on [7]. Intrusion prevention system protects the system from attacks based on node behaviors. Intrusions are detected using data mining (DM) approaches and its main classification is follows: reinforcement learning, regression, classification, optimization, ensemble learning, rule based decision making and clustering [8]. Conventional machine learning approaches and deep learning based approaches have been proposed recently for intrusion detection and prevention [9, 10]. Previous solutions for IDS is designed on the basis of supervised algorithms include K-nearest neighbor (KNN), Support Vector Machine (SVM) [11], Naïve Bayes [12], Random Forest (RF) [13], etc. Likewise the commonly used deep learning algorithms are deep neural network (DNN), long short term memory (LSTM), convolutional neural network (CNN), etc. Deep learning algorithms are time consuming, and complex learning in some cases [14, 15]. Intrusion detection in MANET is a tedious task due to several challenges that are following [16].

1. Selection of packet features to classify nodes into normal and attacker
2. Immediate detection of attackers in network is important to mitigate impact of any malicious activities.
3. Choose algorithm for efficient intrusion detection of any specific intrusion under highly dynamic environment
4. Intrusions detection simultaneously with high detection rate with minimal false positive rate is a challenging.

Hence the best set of packet features result high detection rate, and minimal false positive rate in less detection time. Most of the IDS approaches lead to high false positive rate and low detection rate and also those approaches do not eliminate intrusions completely in network. Feature extraction, selection and transformation are plays the essential role in MANET for intrusion detection. Recently proposed feature extraction and selection techniques considered optimum set of features from all features set based on given test packet, which induces very small detection time to improve the performance of IDP.

Figure 1 indicates the intrusion detection in MANET, where we specified preliminary stages of intruder packets classification. Similar to intrusion detection in MANET, intrusion prevention is also plays significant role to mitigate attacks in MANET since most of the intrusion prevention schemes are insufficient after mobile nodes have been compromised by attacker nodes. Despite of inherent failures in dynamic nature of

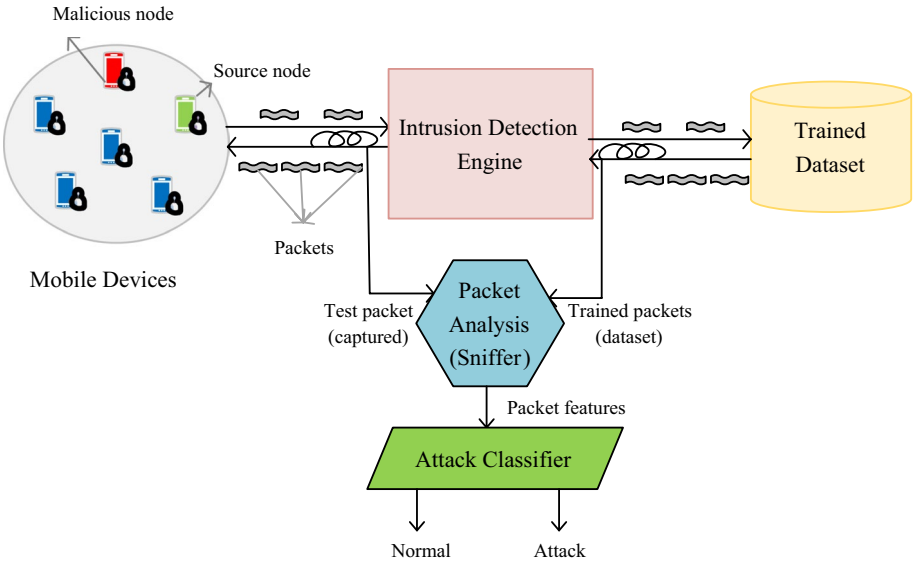


Fig. 1 Intrusion detection in MANET

MANET, conventional cryptography techniques cannot be guarantee to prevent attacks, which leads to high computation expensive and overhead when MANET is highly vulnerable due to security threats [17]. In this paper we proposed a smart approach for Intrusion Detection and Prevention System (SA-IDPS) in MANET. SA-IDPS consists of the following major objectives:

- Design of effective and intuitive IDPS and is suited for real environments with highly dynamic mobility
- To provide immediate response to mobile nodes related to alarm events and to protect the information access.
- Achieve graceful Quality of Service (QoS) while functioning IDPS in MANET
- Propose IDPS model in MANET with high attack detection rate, minimal false alarm rate and overhead

To attain the above mentioned objectives in this paper we provide the complete information of how intrusions detected and prevented in MANET.

Contributions The main contributions of this paper are follows:

- We employed two engines for intrusion detection and prevention, which is referred as IDE and IPE. We propose One Way Hash Chain (SHA-256) for preventing intrusions in MANET through trusted authority
- We consider four units for intrusion detection such as packet analyzer, data preprocessing unit, feature extraction unit, and classification unit.
- In packet analyzer, packet is classified either as normal or attack based on packet header information. Packet features are input variables send to Type 2 Fuzzy Controller (T2FC)

- In data preprocessing, two processes are considered as encoding and logarithmic and linear normalization.
- In feature extraction unit, optimum features are extracted and optimized using Mutual Information (MI) Function, where we extract only optimum set of features for intrusion detection.
- In classification unit, hybrid algorithm is considered for fast intrusion detection. Artificial Neural Network (ANN) is used to train the dataset and Bootstrapped Optimistic Algorithm for Tree Construction (BOAT) is introduced for normal packets and attack packets classification. Attack packets are classified into four classes: DoS, Probe, U2R, R2L and Anomaly. Then we find the attack type either frequent, rare or anomaly. This classification is made by Association Rule Tree (ART).
- We evaluate our SA-IDPS scheme effectiveness using NSL-KDD dataset and tested over NS3 simulation environment and experimental results demonstrate that the proposed scheme provides better results than the previous machine learning techniques.

Paper Organization We have structured our rest of the paper into five sections: Sect. 2 concerns systematic related work on intrusion detection and prevention under MANET with limitations. Sect. 3 details the problem statement where we highlighted the major challenges in recent available works. Section 4 discusses the proposed SA-IDPS in the field of MANET against security attacks. Section 5 demonstrates experiments and results of proposed and well-known previous intrusion detection methods. Section 6 concludes the paper and given future works.

2 Related Work

Over the last few years, enormous IDS methods have been presented to mitigate security attacks in MANET, which are aims at produce accurate attack detection results, but failed to improve the speed of detection and today MANET face several challenges due to security threats such as energy consumption and packet delivery ratio. Hence in this section we address limitations of recent works for intrusion detection and prevention over MANET.

Wahab et al. [18] have presented intrusion detection scheme using SVM over clustered vehicular ad hoc networks. Aim of this ID model is to reduce size of training set for SVM classifier and its advantage is to support for high mobility environment. Various kernel functions are used to test the performance of SVM. Finally the proposed method has proved that it improve the scalability of network with respect to number of nodes (normal and malicious). A drawback of this work is SVM since it failed to tune the parameter set and very complex to obtain better results. Singh and Bedi [19] have discussed multiclass extreme learning machine based Smart Trustworthy IDS with single hidden layer feed forward neural network to categorize nodes into trustworthy, partially trustworthy and malicious in KDD Cup Dataset. There are five agents are used in this paper such as data accumulation agent, preprocessing agent, trust degree computation agent, differentiation agent and decision making agent. ELM has proved that it suitable for intrusion detection in real-time, but it failed to improve the speed of attack detection evaluation. Kolias et al. [20] have proposed IDS to detect most popular attacks on 802.11 using several algorithms (Adaboost, J48, Naïvebayes, OneR, Random Tree, random Forest, ZeroR). Aegean WiFi Intrusion Dataset (AWID) is used in this work and also it is suited for UMTS, LTE, WiMax technologies. It is showed that J48 and random forest classification algorithms provide high

detection rate and low false alarm rate. These two algorithms are simple and ease of use, but it failed to support for large scale datasets. Hence scalability is not achieved. Subba et al. [21] have discussed hybrid IDS with Bayesian game formulation to detect deprivation, flooding, DoS and foraging, blackhole attack, packet dropping attack by using unsupervised association rule mining (ARM) algorithms such as Apriori and Vickrey–Clarke Gorves (VCG). Furthermore a threshold based lightweight module and powerful anomaly based heavyweight module is proposed to obtain lower power consumption. The proposed model is heavyweight and thus it provides low attack detection rate and high false alarm rate. Ahmed et al. [22] have presented a new framework for DoS attack detection using finite state machine (FSM). Intrusion detection system with ad hoc on-demand distance vector (ID-AODV) protocol is proposed, which functions by FSM. There are three operational modules are involving in ID-AODV such as network monitoring, FSM, and DoS detection. In simulation, ID-AODV shows that it obtained better attack detection rate to show high security of mobile nodes in data transmission and collection, but authors does not conveyed about detection delay. Shanthi et al. [23] discussed the concept of intrusion detection and secure key management in MANET using trust metric. For each mobile node direct and indirect is computed and hierarchical group key management is proposed for information access control. Base station is deployed in network for group key generation, distribution and management. Through this work, network lifetime and packet delivery ratio is improved when presence of attackers, but attack detection rate with the use of trust metric is not investigated. Khan et al. [24] discussed about detection and prevention of attackers in network. In order to detect malicious nodes in network, detection and prevention nodes are deployed in network. If it determined any suspicious node, then broadcast this error message throughput the network.

Data packets forwarded by the suspicious node are eliminated in network. For intrusion detection and prevention, more statistical analysis and computation is required. This will results in high overhead and large energy consumption of network. Raja and Ganesh Kumar [25] have proposed a trusted cluster based routing protocol for MANET. A trust management (TM) is concentrated in this paper where they compute a trust value for all mobile nodes. When node has high trust value, then those are considered to be trusted nodes. The goal of this paper is to establish TM based routing protocol to enhance QoS in MANET. Simulation results proved that it obtained better performance for succeeding metrics: energy consumption, throughput, packet delivery ratio, and delay. Mobile nodes behavior is not a constant, which leads to given wrong opinion of someone. Anusha and Sathiyamoorthy [26] discussed an intrusions detection mechanism for MANET using trust based authentication and bio-inspired optimization algorithms. In order to prevent intrusions, certificate authority is deployed in MANET which generates public and private key pair. Deep packet inspection is implemented in this paper to improve MANET security and hence packet features are extracted for deep packet inspection. When attacker is determined in deep packet inspection, error message is send to certificate authority for taking necessary actions. Asymmetric technique can be used for message encryption and signing (validation), but it is very resource intensive and only supported and work well in small messages. Luong et al. [27] proposed a new protocol named as FAPRP, which is expanded as flooding attacks prevention routing protocol. This FAPRP is based on a machine learning approach implemented and tested over MANET. FAPRP is an extended version of AODV routing protocol created to mitigate flooding attacks. Experiments conducted and validated that FAPRP has reached 99% of detection rate for flooding attacks. However, flooding is an initial attack, which easily mitigated through packet header information, but several security attacks are still unsolved in MANET. One research work towards this idea

i.e. detecting new security attacks in MANET is detailed in [28]. In this paper authors have proposed a node collusion method to classify normal and attacker nodes, which intend to mitigate two security attacks: wormhole and sinkhole attacks. For routing attacks prevention, route reserve method is proposed. This work has taken large computational time for nodes classification. Intrusion detection using NSL-KDD dataset is focused on some research works [29–32]. Ahmad et al. [29] studied about the performance comparison of RF, SVM and ELM for network intrusion detection. Each technique applied to detect intrusions with the trained NSL-KDD set. Finally, authors have concluded that ELM is suitable scheme for intrusions detection and validated for large size of dataset. This work tends to increase detection time since processing all preprocessed data with feature extraction and selection is time consuming. Yin et al. [30] tested NSL-KDD dataset using recurrent neural network (RNN) and the performance of RNN is compared with several classifiers such as J48, SVM, RF, and so on. It is supported for binary and multi-class classification. It shows better accuracy rate in intrusion detection. Training time of RNN is higher and hence authors have suggested that, in future long short term memory (LSTM) or gated recurrent unit (GRU) is used to address the issue. Recently, Khan et al. [31] proposed convolutional LSTM and spark ML (machine learning) is proposed for intrusion detection. However, both convolutional LSTM and spark ML require large amount of data for training process and also computations of this combined algorithm is very large. Xu et al. [32] proposed a GRU for network intrusion detection. In this paper, RNN is integrated to GRU for improving intrusion detection performance. Two different datasets are tested such as KDD 99, and NSL-KDD dataset. High total detection rate is 99.42% and 99.31% for KDD and NSL-KDD dataset, respectively. Similarly, they obtained low false positive rate such as 0.05 and 0.84 for KDD 99 and NSL-KDD dataset, respectively. Attack detection rate is very high, but detection time for intrusions becomes very high. It must be less to demonstrate the system has obtained better performance.

3 Problem Statement

In this section, we states the problems existed in the current works. From the review of literature, we come to know that there are still several challenges raised in the design of IDPS in MANET that are follows: (1). Lack of routing attacks detection with low alarm rate, (2). It does not scalable and practical to implement in real-time, (3). It does not sufficient to up-to-date evidences collection, (4). Not tolerant to loss of messages, (5). High message and computation overheads, and (6). It does not automatic and realtime routing recovery.

In [33] authors have proposed a neutrosophic intelligent system (NIS) using self-organized feature maps (SOFM) and genetic algorithm (GA). In neutrosophic system, rules are generated in terms of symbols instead of numerical values. In NIS, attack packets are identified by membership, non-membership, and indeterminacy degrees using SOFM. KDD dataset is tested in this neutrosophic system. GA is used to classify the packets into two classes: normal and abnormal. This paper is proposed generalized neutrosophic set, but it does not suitable for complex applications like intrusion detection. Adaptive fault tolerant mobile agent based IDS is proposed in [34], which tested for KDD dataset. Initially, attacks classification is implemented using TSVID (Trail based classifier using Support Vector Machine for Intrusion Detection) algorithm, NNIDS (Neural Network Approach to Intrusion Detection System), DF-IDS (Determinant Fuzzy system for Intrusion Detection) simultaneously. This work is failed to address of preprocessing issue since it is required to

minimize the false positive rate and increase level of detection rate. TSVID algorithm does not perform well, when we have huge dataset with more noise so it is tricky for decision making. In [35] a new intelligent framework called INDIA, which is referred as intruder node detection and isolation in MANET. There are three processes are invoked in INDIA that are feature extraction, feature optimization and classification. Feature extraction is implemented using trust value (direct trust, indirect trust and total trust) computation for every node. Feature optimization is implemented using particle swarm optimization (PSO). Finally the optimized set of features is classified using NN. The speed of IDS is important element, which is very less in this work and trust computation is implemented itself is does not effective. In [36] a plug and play device was deployed in ad hoc networks which act as packets capture tool. Deep neural network (DNN) was proposed to detect DoS attacks, then convolutional neural network was proposed to detect XSS attacks and long short term memory (LSTM) was proposed to detect SQL attacks. It is implemented using NS2 simulator and tested over KDD Dataset. Plug and play device is cost effective and small power, which leads to low scalability and bringing this tool for IDS, is not practical. In [37] two algorithms are proposed for intrusion detection in networks such as improved PCA (Principal Component Analysis) and Gaussian Naïve Bayes Algorithm. An improved version of PCA minimize data pollution problem. Total number of weighted principal components is 12, which are selected using sequential selection. Feature dimensionality reduction was implemented by enhanced PCA and user behavior is classified using Gaussian Naïve Bayes Algorithm. Runtime of improved PCA is typically large since improved PCA does not select optimum set of features for classification. Gaussian naïve bayes algorithm for packets classification is less but detection rate is not high. In preprocessing, min–max normalization is applied, which is simple algorithm. In this paper, we addressed all abovementioned limitations for improving MANET security. The proposed methods are subsidized in the following section.

4 Proposed Work

In this current section we describe the proposed system for intrusion detection and prevention in detail under mobile ad hoc environment. Figure 2 demonstrates the system architecture for the proposed model.

4.1 System Model

In last few years, researchers have designed intrusion detection and prevention based on conventional approaches, which are not giving predominant results in the aspect of attack detection rate and false positive rate. To mitigate such issues, in this paper we proposed a smart approach for intrusion detection and prevention in mobile ad hoc environment. Our proposed SA-IDPS comprised of Mobile Devices (MDs), Trusted Authority (TA), Packet Analyzer, Preprocessing Unit, Feature Extraction Unit, and Classification Unit. According to the definition of MANET, mobile users are moved rapidly for several locations in ad hoc environment. Network traffic occurs when data packets are received from nearby mobile users. We introduced intrusion detection and prevention engines for mitigating attacks. Packet analyzer will scrutinize the packets based on packet arrival time, num. of packets per flow, packet counts, and packet size from its packet header. Threshold for classifying attack pattern and normal pattern is determined using T2FC, which improves uncertainty

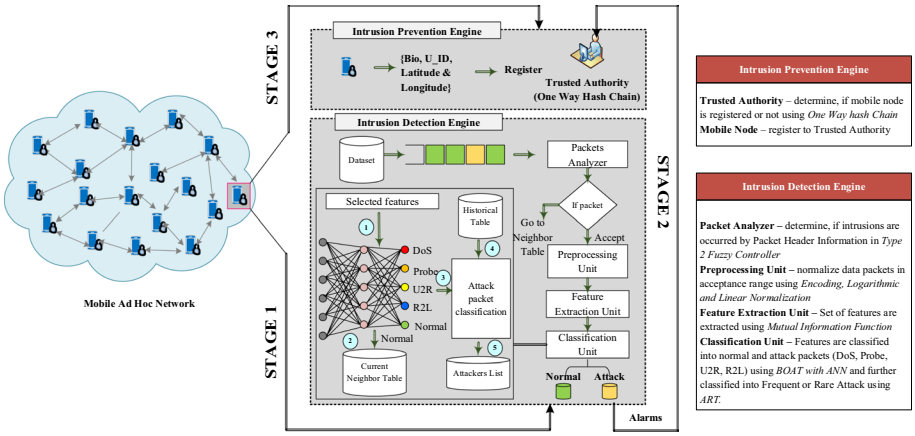


Fig. 2 System architecture for SA-IDS in MANET

while classifying packets. Then attack pattern found packets are forwarded to preprocessing unit, which executes two steps: encoding and normalization. Then normalized packets are forwarded to feature extraction unit, where we extract most optimum set of features, and then classification unit is initiated for packets classification using BOAT with ANN and further it is identified whether rare attack or frequent attack using ART. Trusted authority invoked in this paper for intrusion prevention and hence intrusion prevention engine is used where we generates One Way Hash Chain for each mobile user that fully protect the system from attacker nodes.

4.2 Packet Analyzer

In intrusion detection engine, packet analyzer plays a significant role to find attack pattern in the system. Packets from various locations are obtained in packet analyzer that is processed in intrusion detection engine, which is deployed in network. With the dynamic change of MANET users, packets threshold value may change since constant threshold value does not suitable and it leads to incorrect outcome. So it must be adaptive and required to be dynamic for classify attack patterns. To mitigate this issue, thresholding function is applied and it is computed and updated when each packet is arrival to the intrusion detection engine. For accurate and dynamic thresholding we proposed Shannon Information Entropy is used [38]. The measure of Shannon information entropy is continuous (change the probability value in dynamic way and a small amount of threshold change only when entropy is change by lesser amount). When the result from Shannon information entropy is certainty, then entropy value is zero. Shannon Information Entropy defined by Discrete Random Attribute X with set of results i.e. outputs as: $x_1 \ldots x_n$ and it is calculated by:

$$H(X) = \sum_{i=1}^{n} p(x_i) log_2 \left(\frac{1}{p(x_i)} \right) \tag{1}$$

$$= -\sum_{i=1}^{n} p(x_i) log_2 p(x_i) \tag{2}$$

where $p(x_i) = \Pr(X = x_i)$ represents probability value for ith output of variable X. H can be varied depending upon the spatial and temporal data of mobile devices and it communication to neighbor nodes. Packet header information is verified in each iteration.

In addition to basic packet features from packet header information, node i trust value is computed using following.

$$T_i = \frac{Num.packets\ sent\ sucessfully}{Num.of\ packets\ totally\ sent} \times 100\% \tag{3}$$

where T_i is the trust value of node i, which is computed in percentage. Assume that the number of packets that totally sent by node i is zero, then T_i becomes zero, which means that node i is dropped all incoming packets, who determined as attacker node and this information is broadcasting to nearby neighbors of node i. Total packet features are used in packet analyzer is depicted in Table 1.

The abovementioned features are given as input variables for T2FC, which perform classification for mitigating initial attacks. Type-2 fuzzy system is used to find the various applicability in a rule-based fuzzy systems since uncertainty can be easily modeled. However, type-1 fuzzy sets are not modeled the uncertainty issue. In addition, it minimizes the errors. Primarily, there are four components in T2FC that are fuzzifier, inference engine (Rules), type-reducer and defuzzifier.

Type 2 fuzzy sets are associated with the terms that will appear in Antecedent (if)/Consequent (then) as well as with the input and output of the T2FC. In this system, membership function is used to describe the fuzzy sets.

The main purpose of using T2FC is to resolve uncertainty issue and it can be easily deals with large size of inputs. Footprint of Uncertainty (FOU) is based on the primary membership function of type2 fuzzy set. T2FC can able to process imprecise perception based features. Input and output of Type 2 fuzzy sets for proposed model is following:

- *Input Fuzzy Set* Criteria (see in Table 1) that have taken into account for classification
- *Output Fuzzy Set* Normal or Attack
- *Type 2 Fuzzy Variables* Good, Fair and Poor (Fig. 3).

For generating Fuzzy IF–THEN rules, all available combinations of antecedent fuzzy sets are invoked. Algorithm for packet analyzer is following.

Table 1 Packet header used in packet analyzer

Packet features	Feature name
PF_1	Packet arrival time
PF_2	Num. of packets per flow
PF_3	Packet counts
PF_4	Packet size
PF_5	Packet type
PF_6	Inter-packet interval
PF_7	Flow direction

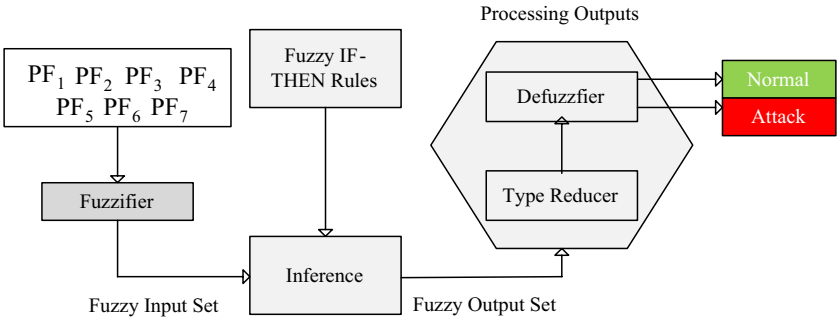


Fig. 3 T2FC running in packet analyzer

Algorithm for Packet Analyzer using T2FC

Step 1) Begin
Step 2) Start T2FC
Step 3) For all packets $p_k \rightarrow (k = 1 \ldots n)$
Step 4) Examine packet features $PF_1, \ldots, PF_7$
Step 5) In T2FC do
Step 6) Transform crisp input to fuzzified input set
Step 7) Generate fuzzy if–then rules
Step 8) Process in Inference Engine
Step 9) Classify input packet based on packet features
Step 10) Examine packet features by Packet Header
Step 11) Check trust value of a node i
Step 12) Compute threshold T for node i packet $p(k)$
Step 13) If $(p_k(v) > T)//p_k(v) =$ value v of packet k
Step 14) Accept packet
Step 15) Else
Step 16) Go to Neighbor Table
Step 17) End if
Step 18) End for
Step 19) End

Consequents of fuzzy if–then rules are given via evaluators. Total number of rules generated for output processing is defined according to input variables. We have taken 7 input variables for classification. Proposed T2FC model has high potential to capture the uncertainties for subjective evaluation. This process is helps to mitigate some attacks such as initial flooding and probe attacks.

4.3 Data Preprocessing Unit

This unit gathers the accepted packets from packet analyzer and preprocesses these packets for classification. The data preprocessing step includes packet encoding, and normalization process that are following.

- *Packet Encoding* It is a new step that we considered in MANET for intrusion detection. In dataset, some features are depicted like abbreviations such as SF, SO, REJ, and RSTO. Before process into feature extraction unit, we transform abbreviation

these features into numerical data. It plays vital role since features can be easily fed into input layer of any type of neural network should be numerical values.

- *Normalization* It is a commonly used step for preprocessing. Min–max normalization is a traditional data preprocessing algorithm, which does not suitable for all cases. Hence in this paper we proposed fast two step normalization techniques in which we execute two normalization steps. (1) Logarithmic: all packet features are converted into acceptable range. (2) Linear: we cap the feature values within 0 and 5. Equations of these steps are following.

$$X_{Normalized} = \log\left(X_i + 1\right) \tag{4}$$

$$X_{Normalized} = (A - B)\frac{X_i - \min\left(X_i\right)}{max\left(X_i\right) - min\left(X_i\right)} \tag{5}$$

where $A = 5, B = 0$.

4.4 Feature Extraction Unit

In feature extraction unit, mutual information is used. We applied MI in preprocessed data. MI is working by Variable Dependence Estimation technique. It is based on both linear and non-linear variables. For this purpose, we have chosen this algorithm for feature extraction and optimization. The traditional definition for MI is follows: "It is a Symmetric Value computed between two Random Variables. It outcomes zero value and non-negative value for MI shows that two variables are independent by each other. Assume that two Continuous Random Variables are follows: $P = \left(p_1, p_2, p_3, p_4, \ldots p_D\right)$ and $Q = \left(q_1, q_2, q_3, q_4, \ldots q_D\right)$ where D is the sum of samples. MI is computed between P and Q are following.

$$MI(P, Q) = H(P) + H(Q) - H(P, Q) \tag{6}$$

where $H(P)$, *and* $H(Q)$ represents information entropies of P and Q

In MI, joint Probability Mass Function $\rho(p, q)$ and Marginal Probabilities $\rho(p)$ and $\rho(q)$ for two discrete variables are computed using following.

$$MI(P;Q) = \sum_{p \in P} \sum_{q \epsilon Q} \rho(p, q) log \frac{\rho(p, q)}{\rho(p)\rho(q)} \tag{7}$$

when we consider MI for features extraction and selection, we must maximize MI between random variables and select the subset of selected features x_S and out variable y and it is defined by following.

$$\tilde{S} = \arg\max_{S} MI\left(x_S, y\right) \quad \text{subject to} \quad |S| = k$$

where k represents the sum of features for optimization.

In order to deal with optimization problem, we considered greedy solution. Here subsets of features are selected in incremented way. i.e. one feature at a time.

4.5 Classification Unit

Classification plays very important role to find the intrusion in the network traffic. Determination of accuracy and detection performance of intrusion detection is mainly based on the selection of best classifier algorithm and the goal of the classifier algorithm is to construct a concise and precise model that can be used to predict the intrusion from the real-time network traffic. In this paper we presented a dynamic and hybrid model for packets classification. A hybrid model is the combination of two algorithms BOAT and Neural Network.

BOAT classifier is identified to detect the misuse attacks in MANET. It can be adapted to the unique characteristics of MANET and also solve the energy-constrained issues because BOAT can use only two scans to build several levels of the tree over the huge training dataset, resulting in an average performance of three times better than the existing classification algorithms. BOAT also has ability to update the decision tree with respect to the dynamic insertion or deletion of the node from the network topology to solve one more important issue in MANET i.e. dynamic topology or mobility. BOAT does not require any storage to write the temporary data and needs low run-time resources. A traditional process for BOAT can be seen in Fig. 4.

In classification unit, BOAT is used for classification and neural network is used to train the dataset for classification into normal, and attack packets (DoS, Probe, U2R, and R2L). Firstly neural network is applied to weight the subset of features in previous unit i.e. feature extraction unit. The BOAT classifier is extracted in trained NN. Most suitable BOAT classifier is used to construct the decision tree using trained neural network. In Fig. 4, the BOAT verifies the real-time network packets with each and every decision splitting criterion whether the network packet is authorized or intrusion type. If any network packet is matched with splitting decision criterion, it will be considered as an intrusion. The algorithm immediately stops the verification process and informs the intrusion name, type with its severity to respective authority to take proper decision. If match is not found until the last best splitting criterion N, the network packets are passed to anomaly detector for further verification.

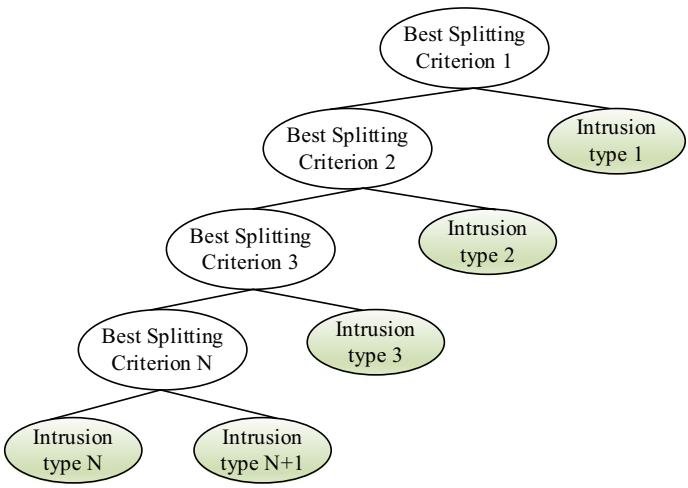


Fig. 4 Decision making process of BOAT classifier

4.5.1 ART Based Classification

Decision tree rules are again modeled using ART for further classification. Association rules are generated and accepted for next iteration. In historical table, we keep the simulated packets data of nodes in past and future behavior data. Figure 5 shows the classification workflow.

The following features are keeps stored in historical table

1. Num. of packets sent or total num. of communications
2. Num. of packets delivered successfully within time interval
3. Num. of dropped packets rate
4. Average throughput
5. Packet transmission rate
6. Hop count
7. Num. of mis-transmitted packets
8. Trust values
9. With the information of packet features listed above, we classify the attack is frequent or rare.

4.6 Intrusion Prevention

Several real-time applications related to MANET security are video streaming, file transfer, etc. Intrusion prevention is important to restrict the access for malicious nodes arrived in the network [39, 40]. For intrusion prevention, we proposed One-Way Hash Chain Function. It can be used in many network security applications and also good for authentication by generate hash values. Intruders can generate fake or spoofed identities from legitimate nodes for the

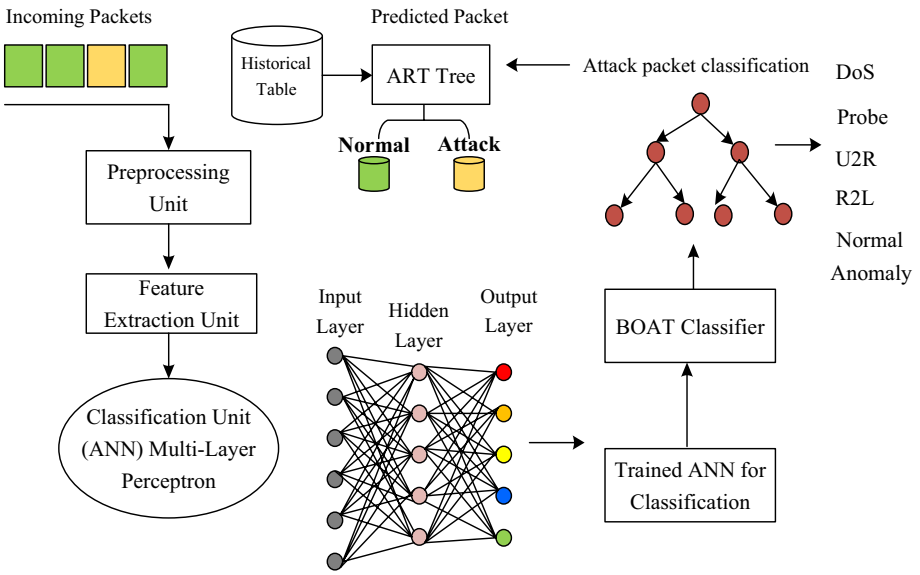


Fig. 5 Hybrid algorithm workflow

intention to disrupt the IDS or try to make communication between legitimate nodes to gain data packets. It could be direct when mobile nodes use Asymmetric Cryptography algorithm or Digital Signatures for authentication, but it protects packets from being tampered by attackers. Due to large computation overhead and computations required to generate public key, in this paper we proposed one-way hash function. However asymmetric algorithm does not suitable for resource constrained devices similarly does not supported in distributed computing environment. Likewise, Symmetric algorithms execute 3 to 4 orders of magnitude (faster) than Asymmetric Cryptography technique. Currently authors have used this one-way hash chains to safeguard network against malicious attacks (DoS, and resource consumption). Both are frequent attacks in MANET. Working of hash function is illustrated in following.

A One-Way Hash Function has been build using Hash Function (h), which mapping with a variable length input to a fixed length string by:

$$h : (0,1)^* \rightarrow (0,1)^{\alpha} \tag{8}$$

where α is the output length hash function (in bits) e.g. SHA-1 and MD-5. Most important properties of hash function h is follows:

- h is taken as an input function at any packet size (output is stable size)
- It will be very simple to calculate hash function h for input O
- It use One-Way Hash property for making $h(O)$
- $h(O)$ always has Collision-Free property since it does not gives any identical outcome for 2 or more inputs.

For applying one-way hash function, a mobile node chooses random variable $r \in (0,1)^{\alpha}$ and calculates list of values using r $(\mathrm{H}_0, \mathrm{H}_1, \mathrm{H}_2, \mathrm{H}_3, \ldots \mathrm{H}_n,)$ where $\mathrm{H}_0 = r$ and $\mathrm{H}_i = h(\mathrm{H}_{i-1})$ for $0 < i \leq n$. For hashing, we used SHA-256. Therefore hash function for node i is computed by following.

$$h_i = \langle B, U - ID, LA, LO \rangle \tag{9}$$

where h_i is the hash function for authenticating node i to the TA, B is the biometric (finger vein), User Identifier (U-ID), and Latitude (LA) and Longitude (LO). Finger vein is one of the unique biometric considered for authentication purpose. We extract features from user finger vein and processed for hash generation.

5 Experimental Results

In this section, we studied about experiments conducted in the proposed scheme to evaluate the performance. We used NSL-KDD dataset for testing the performance. Then we presented the definition of each evaluation metrics. Finally we compared the performance of the proposed scheme with other well-known previous works.

5.1 Experiment Settings

Our proposed scheme is implemented in NS3 simulation environment running over Ubuntu OS. Zhang [41] and Feng et al. [36] have tested NSL-KDD dataset in MANET using NS3 (3.26 version).

In this paper we consider similar simulation environment for testing dataset with various security attacks. Initially, we deploy 50 mobile nodes randomly in 1000 m*1000 m simulation area. Simulation parameters used in this paper is illustrated in Table 2. Figure 6 shows the simulation environment for mobile nodes deployed in certain region. Figure 7 a shows the result for intrusion prevention in trusted authority using one-way hash function, and Fig. 7b shows the mobile nodes connection. Figure 8 illustrates the data transmission between mobile nodes and finally Fig. 9 shows the tested dataset i.e. NSL-KDD dataset considered while simulation (KDDTest.arff and KDDTrain.arff files) (Table 3).

5.1.1 NSL-KDD Dataset Description

It is an extended version of dataset created for intrusion detection. It limits the problem of KDD Cup 99 dataset. The major limitation of KDD Cup 99 is redundancy and duplicate copies of information i.e. 78% for training and 75% for testing set. Other limitation is non-uniform distribution for target classes, which cause poor results in classification. We tested all features for dataset to classify attacks. There are four classes of attacks are presented in NSL-KDD Dataset as follows:

- *Denial of Service (DoS)* This type of attacker invokes several operations such as targeting memory resources, or restricts authorized users access. E.g. Syn Flood
- *Remote to Local (R2L)* This type of attacker can able to forward packets to adjacent legitimate nodes without the knowledge of the particular node. E.g. remote buffer overflow and guessing password attacks.
- *User to Root (U2R)* This type of attackers has permission to use legitimate nodes and then they exploit certain threats to get access for super user. E.g. local buffer overflow attacks.

Table 2 Simulation parameters in NS3 environment

Simulation parameter	Choice
Simulation area	1000 m*1000 m
Number of nodes	50
Node mobility model	Random waypoint model
Node speed (Max)	5 m/s
Forwarding capacity	2 Mbps
Transmission range	250 m
Number of flows	50
Packet transmission average rate (per flow)	512 bytes/packet, packet/s
Node buffer size	64 packet (fixed)
Nodes distribution	Random
Traffic type	TCP, UDP, and ICMP
Queue type	Priority queue
Interface type	Physical wireless
Duration for packets carrying	1 s
Neighbor nodes waiting time	0.3 s
Propagation delay mode	Constant speed
MAC type	Ad Hoc Wi-fi MAC

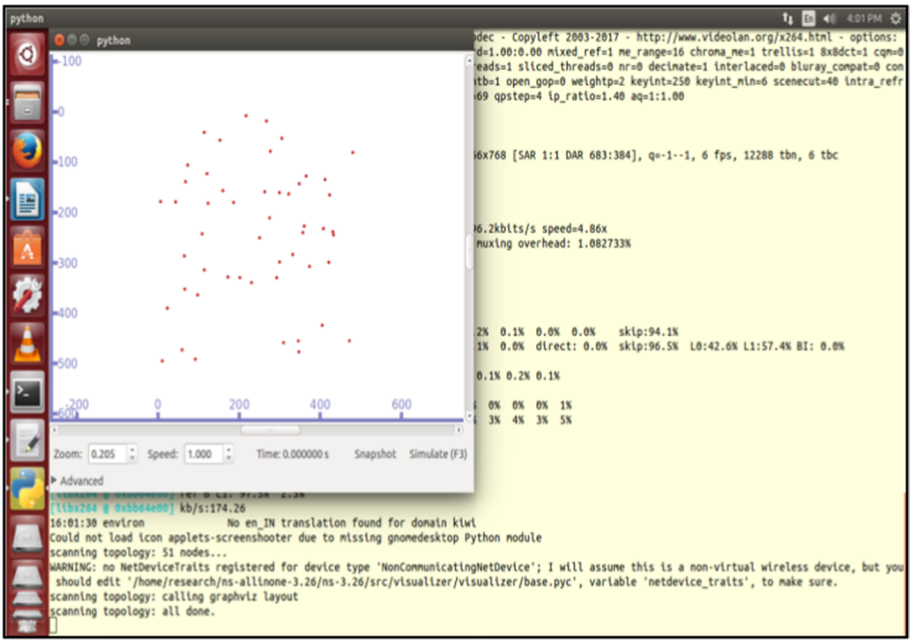


Fig. 6 Simulation environment for MANET

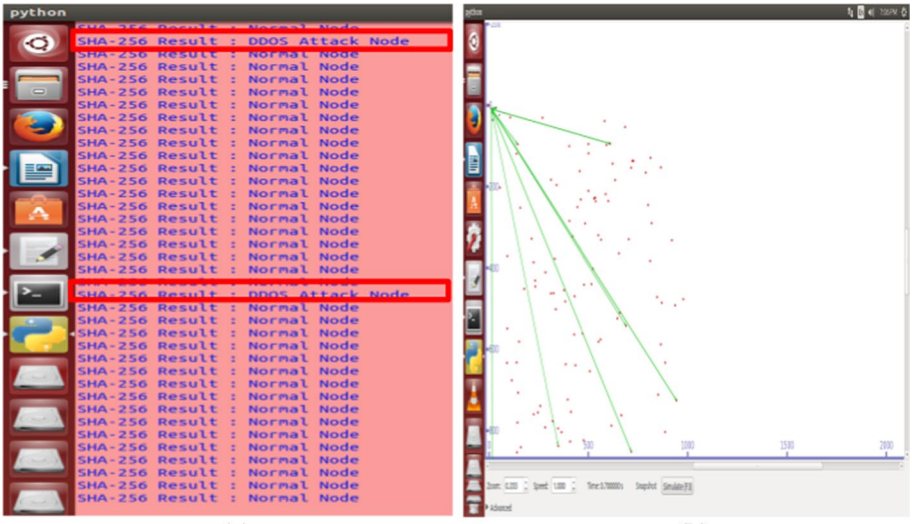


Fig. 7 **a** Intrusion prevention result and **b** nodes connection

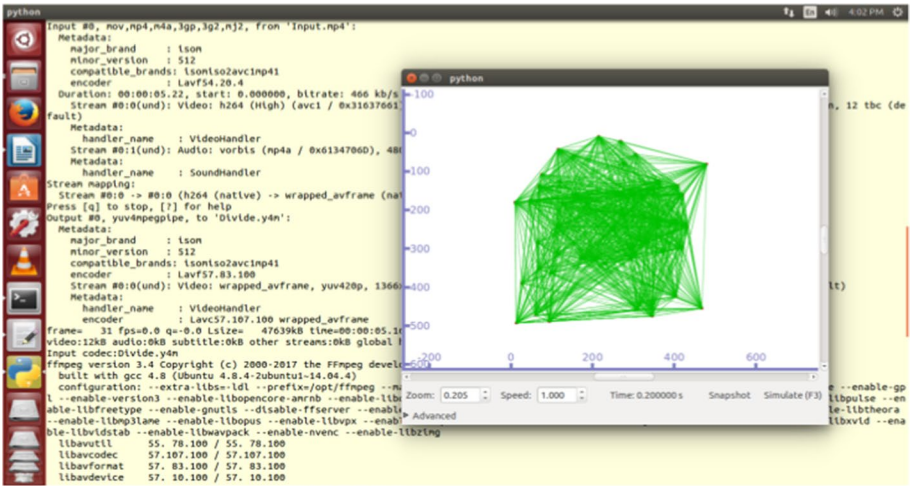


Fig. 8 Data transmission among nodes

Fig. 9 NSL-KDD dataset

- *Probing* This type of attacker collect data of the entire network to make several security threats. E.g. port scanning attack.

The list of features for NSL-KDD dataset according to its type (continuous and discrete) is illustrated in Table 4.

Among 41 features set, 38 features are numeric and 3 features are non-numeric (protocol type, service type and flag). In addition, 1–10 features are basic features, 11–22 are content features and 23–41 are traffic features and 1 class label for each entry, illustrated in Table 4. Each entry in dataset in consists of 41 packet features and the details of attacks and total number of attacks for each class is listed in Table 5. Table 6 consists of attack types for four classes of 41 features are illustrated. In our testing set, we

Table 3 Neural network parameter set

Symbol	Parameter	Description	Value used
LR	Learning rate	It is used to adjust weight values at each round (range between 0 and 1)	0.3
MO	Momentum	It is used to adjust weight values in back propagation to enhance convergence speed and eliminate local optima (range between 0 and 1)	0.2
NE	Number of epochs	Sum of epochs or passes via training data	600
v	Validation in percentage	The percentage of the validation set from training data	20%
S	Seed	Seed is considered for random number generator. Random numbers are used for setting initial weight value for connections between nodes (range between greater than or equal to zero)	0
HL	Hidden layer	Number of features processed in hidden layer	25
δ	Threshold	Threshold for consecutive errors considered in validation testing.	20

Table 4 NSL-KDD dataset description

F#	Feature name	Feature type	Description
1	Duration	Continuous	Time duration of network connection
2	Protocol_Type	Discrete	Type of protocol is used for making connection e.g. tcp
3	Service	Discrete	Type of network service is used in the destination e.g. ftp-data
4	Flag	Discrete	Connection status either normal or error
5	Source_Bytes	Continuous	Sum of bytes (packet) sent from sender to receiver at single_connection
6	Destination_Bytes	Continuous	Sum of bytes received at single_connection from sender node
7	Land	Discrete	When IP addresses and port numbers of sender and receiver is same, it represents value 1 otherwise 0
8	Wrong_Fragment	Continuous	Sum of wrong fragments during connection
9	Urgent	Continuous	Sum of emergency packets, ready to transmit
10	Hot	Continuous	Sum of hot pointers displayed in the packet
11	Num_Failed_Logins	Continuous	Sum of attempts for failed login
12	Logged_in	Discrete	It denotes login status: 1 (for successful connection) and 0 otherwise
13	Num_Compromised	Continuous	Sum of negotiated conditions
14	Root_Shell	Continuous	It represents whether root shell is obtained or not (1 = yes, 0 = otherwise)
15	Su_Attempted	Continuous	Su-Root obtained or not (1 = obtained and 0 = otherwise)
16	Num_Root	Continuous	Sum of root access and operations is considered as root during connection.
17	Num_File_Creations	Continuous	Sum of file creation operations during connection.
18	Num_Shells	Continuous	Sum of shell-prompts
19	Num_Access_Files	Continuous	Sum of operations on access-control files
20	Num_Outbound_Cmds	Continuous	Sum of outbound commands during ftp-session
21	Is_Host_Login	Discrete	Login status (1 = hot login, else 0)
22	Is_Guest_Login	Discrete	Login guest status (1 = hot list, else 0)
23	Count	Continuous	Sum of connections to the same receiver for last 2 s
24	Srv_Count	Continuous	Sum of connections requested for same service i.e. port number

Table 4 (continued)

F#	Feature name	Feature type	Description
25	Serror_ Rate	Continuous	The amount of connections (in percentage) that activates the flag among the connections grouped in count (srv_count = 23)
26	Srv_Serror_Rate	Continuous	The amount of connections (in percentage) that activates the flag (REJ) among the connections grouped in count (srv_count = 24)
27	Rerror_Rate	Continuous	The amount of connections (in percentage) that activates the flag (REJ) among the connections grouped in count (srv_count = 23)
28	Srv_rerror_Rate	Continuous	The amount of connections (in percentage) that activates the flag (REJ) among the connections grouped in count (srv_count = 24)
29	Same_Srv_Rate	Continuous	The sum of connections (in percentage) that requested same service connections grouped in count (srv_count = 23)
30	Diff_Srv_Rate	Continuous	The sum of connections (in percentage) that requested different service connections grouped in count (srv_count = 23)
31	Srv_Diff_Host_Rate	Continuous	The sum of connections (in percentage) that requested different receiver node connections grouped in count (srv_count = 24)
32	Dst_Host_Rate	Continuous	Sum of connections have same receiver IP address
33	Dst_Host_Srv_Count	Continuous	Sum of connections (in percentage) consists of same port number Sum of connections (in percentage) consists of same port number
34	Dst_Host_Diff_Srv_Rate	Continuous	Sum of connections (in percentage) requested same service connections grouped in count (Dst_Host_Count = 32)
35	Dst_Host_Same_Srv_Rate	Continuous	Sum of connections (in percentage) requested different service connections grouped in count (Dst_Host_Count = 32)
36	Dst_Host_Same_Srv_Port_Rate	Continuous	Sum of connections (in percentage) requested same sender port connections grouped in count (Dst_Host_Srv_Count = 33)
37	Dst_Host_Srv_Diff_Host_Rate	Continuous	Sum of connections (in percentage) requested different sender port connections grouped in count (Dst_Host_Srv_Count = 33)
38	Dst_Host_Serror_Rate	Continuous	Sum of connections (in percentage) initiated for flag (S0, S1, S2, and S3) grouped in count (Dst_Host_Count = 32)

Table 4 (continued)

F#	Feature name	Feature type	Description
39	Dst_Host_Srv_Serror_Rate	Continuous	Sum of connections (in percentage) initiated for flag (S0, S1, S2, and S3) grouped in count (Dst_Host_Srv_Count = 33)
40	Dst_Host_Rerror_Rate	Continuous	Sum of connections (in percentage) initiated for flag (REJ) grouped in count (Dst_Host_Count = 32)
41	Dst_Host_Srv_Rerror_Rate	Continuous	Sum of connections (in percentage) initiated for flag (REJ) grouped in count (Dst_Host_Srv_Count = 33)
42	Class_Label	Discrete	Type of attack (DoS, Probe, R2L, U2R or Normal)

Table 5 Total number of attacks

Dataset	DoS	Probe	R2L	U2R	Normal	Total
KDDTrain^{+}	45,927	11,656	995	52	67,343	125,973
KDDTest^{+}	7460	2421	2885	67	9711	22,544
KDDTest^{-21}	4344	2402	2885	67	2152	11,850

Table 6 Type of attacks for attack classes

Attack class	Num_ of_ Attacks	Attack type
DoS	10	Land, Nepune, Pod, Teardrop, Back, Apache 2, UDPstrom, Worm, Processtable, Smurf
Probe	6	Ipsweep, Satan, Portsweep, Mscan, Nmap, Saint
R2L	16	Guess_password, Named, Sendfmail, Ismap, Snmapgetattack, Waremaster, Xlock, Xsnoop, Http_Tunnel, Phf, Waremaster, Spy, Xlock, Warezclient, Ftp_Write, Multi-hop
U2R	7	Ps, Perl, Rotkit, Loadmodule, Buffer-Overflow, SQLattack

comprised of particular attack types that disappear in the training set, which intend to perform more theoretical and realistic simulation for intrusion detection.

5.2 Evaluation Measures

In this section we present the evaluation measures of the proposed model. The following performance metrics are considered for evaluation.

(a) *Accuracy* It is one of important performance metric for evaluating intrusion detection system. It is defined as the sum of packets classified correctly than total number of packets sent. It is written by:

$$Accuracy = \frac{TP + TN}{TP + FP + FN + TN} \tag{10}$$

where TP is the true positive, TN is the true negative, FP is the false positive and FN is the false negative.

(b) *Attack Detection Rate* It is computed by the rate of TP, which is defined the sum of packets classified correctly as anomaly than total number of packets sent.

$$ADR = \frac{\#of\ detected\ attacks}{\#of\ attacks} \times 100\% \tag{11}$$

(or)

$$ADR = TPR = \frac{TP}{TP + FN} \tag{12}$$

(c) *False Positive Rate* It is calculated by the sum of packets classified wrongly as anomaly than total number of packets sent.

$$FPR = \frac{\#of\ misclassified\ processes}{\#of\ normal\ processes} \times 100\% \tag{13}$$

(d) *Detection Delay* It is the sum of time for detecting attack in packets from the starting to the ending time.

$$DD = AD_{ST} - AD_{ET} \tag{14}$$

In following we discuss about QoS metrics in MANET since QoS is one of the emerging issues in MANET, which must be addressed in intrusion detection.

(e) *Packet Delivery Ratio* It is defined as the ratio of packets delivered to the destination successfully in network to the total number of packets sent from the source node.

$$PDR = \frac{Num.of\ packets\ delivered\ sucessfully}{Num.of\ packets\ sent} \times 100 \tag{15}$$

(f) *Throughput* In MANET, packets delivered through certain physical/logical links. Packets forward through a certain adjacent nodes. It is estimated in bits per second (bit/s or bps) or can be measured as data packets per second or per time slot.

$$Throughput = \sum_{i=1}^{n} NPR / \sum_{i=1}^{n} NPS \times Num\_H \tag{16}$$

where *NPR* is the number of packets received, *NPS* is the number of packets sent, and *Num_H* is the number of hops.

(g) *Energy Consumption* It is the necessary metric to deliver one packet on each iterations. Energy consumption (EC) in each node is given as follows.

$$EC = E_{Adv} + E_{Dis} + E_{Syn} + E_{Res} \tag{17}$$

where E_{Adv} is the energy consumption rate for advertising packets, E_{Dis} is the energy consumption rate for discovering packets, E_{Syn} is the energy consumption rate for synchronizing packets, and E_{Res} is the energy consumption rate to respond the packets.

5.3 Comparative Study

In this current section, we present the comparison of our proposed SA-IDPS model with well-known previous works to show that our proposed model is efficient in terms of intrusion detection and QoS based metrics. Comparison made with the following four previous works: Elwahsh et al. [33], Vimala et al. [34], Kavitha et al. [35], and Feng et al. [36]

Table 7 shows theoretical comparison among previous works based on advantages and limitations. To overcome the limitations of previous works, in this paper we proposed a smart approach for intrusion detection and prevention. Table 8 shows the advantages of our proposed model

5.3.1 Results and Discussion

In this section we discuss experiment results for the proposed model and previous works including, Elwahsh et al. [33], Vimala et al. [34], Kavitha et al. [35], and Feng et al. [36]. Plotting graphs for the comparison and investigation is following.

Table 7 Summary of the state-of-the-art approaches

References	Methods	Contributions	Advantages	Limitations
Elwahsh et al. [33]	NIS, SOFM, and GA	In neutrosophic system is proposed to test KDD dataset by methods: GA and SOFM	Effective for simple real-world applications Effective against end-to-end communication	Uncertainty issue is not solved Not suitable for complex applications (particularly intrusion detection)
Vimala et al. [34]	SVM, fuzzy logic and NN	Three methods are used for packets classification. Finally proved that SVM outperforms than the fuzzy logic and NN	Widely used classifier among machine learning algorithms Flexible in features selection	Higher false positive than other two methods It is difficult to process for large scale dataset
Kavitha et al. [35]	Trust computation, PSO and NN	There are three processes are involving: feature extraction, selection and classification	Efficient in determine the number of nodes attacked Internal and external protection by preserving attackers in network	IDS speed is important metric, which is very less and trust computation is not updated by any third party
Feng et al. [36]	Plug and play device, DNN, and LSTM	Capture tool (plug and play device) is deployed in MANET for classification	Three different attacks detected in real-time Support for independent environment	Plug and play device is cost effective and resource constrained For long computation, it might be dead

Table 8 Advantages of the proposed model

Algorithm	Advantages
Packet analyzer (type 2 fuzzy controller)	It avoid initial attacks such as probe and flooding and completely addressed uncertainty issue
Preprocessing unit (encoding and logarithmic normalization)	It helps in improving attack detection rate and reducing false positive rate
Feature extraction unit (mutual information)	It determines optimum set of features for classification process
Classification unit (BOAT + DNN + ART)	It consumes less time for classification since we use BOAT with DNN for initial classification (Normal/Attack) and then classified it further into rare and frequent using ART
One way hash chain (intrusion prevention)	It support for protecting the network from internal and external attackers and maintains network security and mobile users privacy

5.3.1.1 Effectiveness for Accuracy Accuracy performance of the proposed intrusion detection and prevention model and the comparison with previous works is depicted in Fig. 10

Figure 10 shows that comparison of accuracy with respect to number of attacks for the proposed model and four well-known previous works. From this graph, we can see that our proposed model have higher accuracy when compared to four previous works. These provide poor results when presence of intruders such as DoS, U2R, R2L, and probe. Preprocessing, feature extraction and classification are essential steps for intrusion detection and trust management in MANET can be improved and preserved the network from intrusions. Previous works are failed to propose effective algorithms for these steps. Experimental results demonstrate that our proposed smart approach model provides effective results on both frequent and rare attacks with the use of historical table management, efficacious preprocessing, feature extraction and classification steps. Hence, it can determine any kind of security attack in MANET and to conclude our proposed SA-IDP model is secured and protected from intruders than previous works.

5.3.1.2 Effectiveness for ADR In this paper, we proposed a new combination of algorithms for classifying packets in different aspects. We firstly classify packet into normal or attack. If the packet is attack, then we identify whether attack is frequent or rare attack. Figure 11 indicates the performance of ADR with respect to number of attacks.

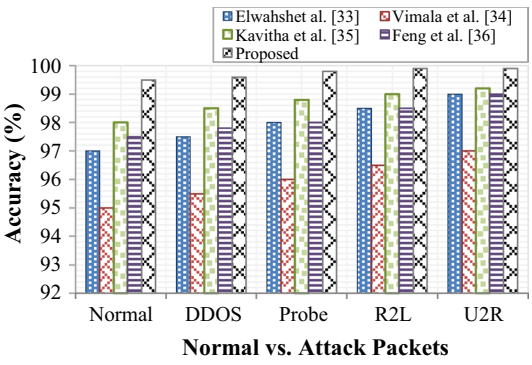


Fig. 10 Results for accuracy

We compare our proposed model with previous works in MANET environment. ADR can be varied according to number of packets and number of nodes arrived in the network. Our proposed model reaches high detection rate for any type of class (normal/attack). The average ADR is 99.4%, which is relatively higher than the previous works, such as 97.5%, 94.52%, 98.36%, and 97.86% for Elwahsh et al. [33], Vimala et al. [34], Kavitha et al. [35], and Feng et al. [36], respectively. In this paper, we invoke trusted authority (one-way hash function) for intrusion prevention, which restricts the access of malicious nodes. It helps to improve ADR when presence attackers. In previous works, legitimate nodes can be easily compromised by intruders and get packets and have full of rights to access the system.

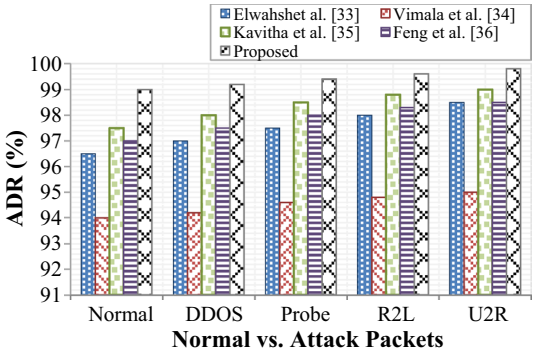
5.3.1.3 Effectiveness for FPR In general, FPR is an outcome (event) is incorrectly found by the intrusion detection system as being an intrusion when none of the malicious activity has occurred. Therefore, objective of FPR should be minimizing these wrong identifications by assumptions. These incorrect predictions have occurred at many more in previous works. Hence optimum set of features must be taken into account for intrusion detection. Previous works are failed in this constraint. Experiment results for FPR represents that the proposed model leads to minimal FPR when compared to previous works. This is due to that proper optimization of features for classification using Mutual Information, where we can accurately get the optimum set of features for intrusion detection (Fig. 12).

5.3.1.4 Effectiveness for Detection Delay Detection delay is important when designing intrusion detection since timely detection of attacks may prevent the network by any abnormal activities and loss. Our proposed model considers this criterion while developing intrusion detection and it is suitable for real-world applications.

Figure 13 indicates the performance comparison of detection delay for the proposed and previous works. Detection delay is a negative indicator, which must be less to show the system has achieved high performance. Graph clearly represents that the number of nodes increases then detection delay is also increase. In this graph, we show the performance of scalability achievement of our proposed model in MANET environment. The average detection delay for the proposed model is 0.09 s and the previous work has taken 0.118 s, 0.3 s, 0.2 s, and 0.54 s for Elwahsh et al. [33], Vimala et al. [34], Kavitha et al. [35], and Feng et al. [36], respectively.

5.3.1.5 Effectiveness for PDR PDR is most significant metric for improving QoS in MANET environment. In this paper we focus on this metric for intrusion detection.

Fig. 11 Results for ADR



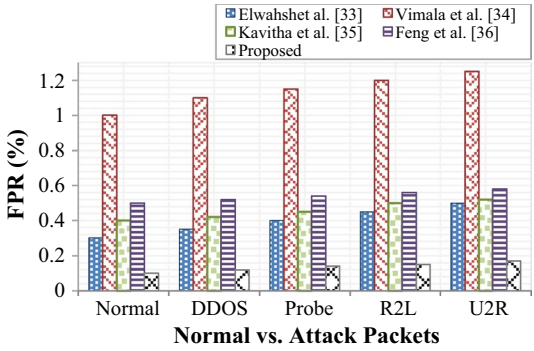


Fig. 12 Results for FPR

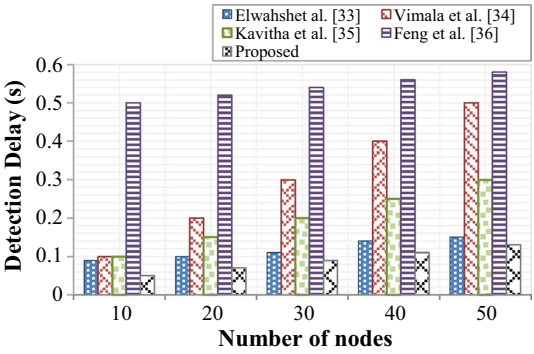


Fig. 13 Results for detection delay

When select most trusted one in network, we can achieve high PDR. Hence in this paper we consider historical table to store nodes behavior, which is updated on the basis of time interval. The graphical representation for PDR with respect to number of nodes is depicted in Fig. 14. Typically, when number of nodes increases, the PDR is gradually decrease. The graphical results illustrate that our proposed model is decrease in minimum level i.e. 100–90% only. When we perform simulation for previous work, Feng et al. [36] only have obtained better PDR than others because they deployed packet capturing tool named as plug and play device, which improves number of packets transmission to destination node. Our proposed model obtained the average PDR of 96% for 50 nodes, which is higher than previous works.

5.3.1.6 Effectiveness for Throughput It is defined as the successful packets transmission rate than previous works. It is a positive indicator so it must be higher to show the system has obtained better performance. Figure 15 shows the result for throughput with respect to number of nodes.

In previous work [36] authors proposed DNN for DDoS attack detection which result higher throughput, which is the first better existing work, compared to our proposed model. We combine DNN with BOAT and ART algorithms for effective classification. In other previous works, throughput decreases and does not suitable for intrusion detection under large scale network environment. Experiment results shown that the proposed model has obtained the average of throughput in 220kbps which is higher than previous works.

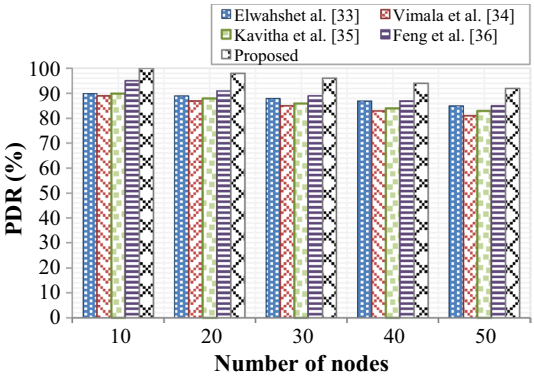


Fig. 14 Results for PDR

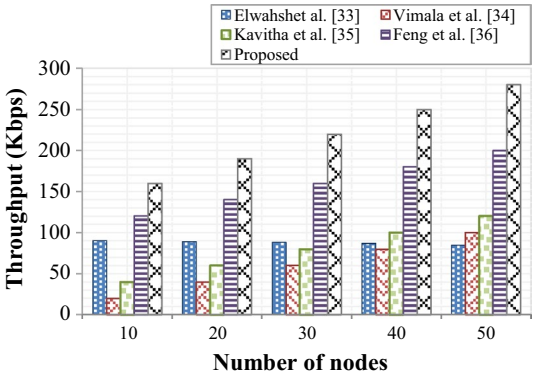


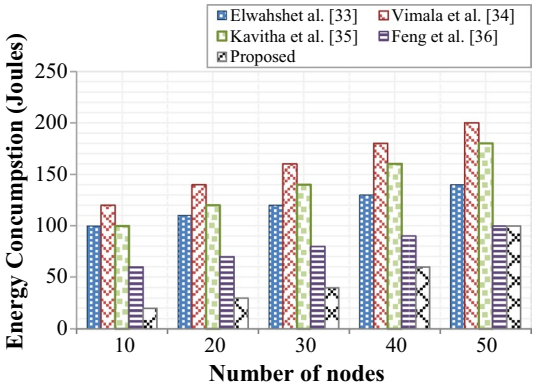
Fig. 15 Results for throughput

5.3.1.7 Effectiveness of EC Consideration of energy to acquire better QoS in intrusion detection is the significant part of this paper, because mobile devices are resource constrained recently. We reduce the rate of energy consumption by proposing novel and hybrid algorithm. We demonstrate the result for EC for the proposed model and previous works in Fig. 16. From the experiment results, it is clear that the proposed model has required minimum amount of energy to perform intrusion detection operation. In this paper we proposed one-way hash function for authenticating users to trusted authority. Intrusion detection engine is faster to reply for a node regarding the current received packet is normal or attack. For this we proposed normalization, feature extraction, packet analyzer and effective classification operation.

The average rate of EC for the proposed model is 50joules which is minimum than previous works.

Table 9 illustrates the average comparison for the proposed model and previous works in terms of accuracy, ADR, DD, FPR, PDR, throughput and EC. Finally the experimental results are shown that our proposed model is more efficient and accurate on both intrusion detection and prevention in MANET.

Fig. 16 Results for EC



6 Conclusion and Future Work

Security in MANET concerns open-up space for researchers to extend their research from traditional to new schemes. When compared to traditional approaches, security in MANET brings some other research issues for IDPS. Hence we focused on previous MANET IDPS and determined research gaps include poor scalability, inadequate QoS, access control for unauthorized access, and avoid legitimate nodes compromise, etc. In this paper, we presented a new approach called as SA-IDPS in MANET. SA-IDPS mobile nodes are deployed in specific region. We registered each mobile node to TA by biometric, U-ID, and latitude and longitude. One way hash chain is applied here and hence intrusions are prevented. In intrusion detection, packet analyzer has helped to determine whether intrusions are occurred. It will be operated using T2FC and packet header information. Data normalization and encoding processes are held in preprocessing unit. In feature extraction unit, optimum set of features are extracted and gathered for next step i.e. classification. BOAT with ANN is helped us to improve attack detection rate and minimal false alarm rate. If classified packet is identified as attack packet, it is further classified into frequent attack or rare attack, which is implemented using ART. Experimental results has proved that the proposed SA-IDPS meets the security required in MANET and mitigate four different attacks such as DoS, Probe, U2R, and R2L. In future we have planned to work on other new security attacks in MANET and also tested for large size of real world dataset.

Table 9 Numerical comparison results (average)

References	Accuracy (%)	ADR (%)	FPR (%)	DD (s)	PDR (%)	Throughput (kbps)	EC (J)
Elwahsh et al. [33]	98	97.5	0.4	0.118	87.8	87.8	120
Vimala et al. [34]	96	94.52	1.14	0.3	85	60	160
Kavitha et al. [35]	98.7	98.36	0.458	0.2	86.2	80	140
Feng et al. [36]	98.16	97.86	0.54	0.54	89.4	160	80
Proposed	99.74	99.4	0.136	0.09	96	220	50

References

1. Islabudeen, M., & Kavitha Devi, M. K. (2015). An efficient intrusion detection system with BOAT classifier to detect rare and frequent misuse attacks in MANET. *International Journal of Applied Engineering Research, Research India Publications, 10*(55), 2633–2639.
2. Chaudhary, A., Tiwari, V. N., & Kumar, A. (2016). Design an anomaly-based intrusion detection system using soft computing for mobile ad hoc networks. *International Journal of Soft Computing and Networking, 1*(1), 17.
3. Meddeb, R., Triki, B., Jmili, F., & Korbaa, O. (2018). An effective IDS against routing attacks on mobile ad hoc networks. *Frontiers in Artificial Intelligence and Applications*, *303*, 201–204.
4. Vegda, H., & Modi, N. (2018). Secure and efficient approach to prevent ad hoc network attacks using intrusion detection system. In *2018 Second international conference on intelligent computing and control systems (ICICCS)*.
5. Sankaranarayanan, S., & Murugaboopathi, G. (2017). Secure intrusion detection system in mobile ad hoc networks using RSA algorithm. In *2017 Second international conference on recent trends and challenges in computational models (ICRTCCM)*.
6. Abbas, S., Faisal, M., Rahman, H. U., Khan, M. Z., Merabti, M., & Khan, A. R. (2018). Masquerading attacks detection in mobile ad hoc networks. *IEEE Access, 6,* 55013–55025.
7. Borkar, A., Donode, A., & Kumari, A. (2017). A survey on intrusion detection system (IDS) and internal intrusion detection and protection system (SA-IDPS). In *2017 International conference on inventive computing and informatics (ICICI)*.
8. Salo, F., Injadat, M., Nassif, A. B., Shami, A., & Essex, A. (2018). Data mining techniques in intrusion detection systems: A systematic literature review. *IEEE Access, 6,* 56046–56058.
9. Nishani, L., & Biba, M. (2015). Machine learning for intrusion detection in MANET: A state-of-the-art survey. *Journal of Intelligent Information Systems, 46*(2), 391–407.
10. Singh, D., Devendra, K., & Bedi, S. (2015). A survey: Feature based intrusion detection system in mobile ad-hoc network. *International Journal of Computer Science and Technology, 6,* 135–140.
11. Shams, E. A., & Rizaner, A. (2017). A novel support vector machine based intrusion detection system for mobile ad hoc networks. *Wireless Networks, 24*(5), 1821–1829.
12. Veeraiah, N., & Krishna, T. B. (2019). Trust-aware FuzzyClus-Fuzzy NB: Intrusion detection scheme based on fuzzy clustering and Bayesian rule. *Wireless Networks, 25,* 1–11.
13. Resende, P. A. A., & Drummond, A. C. (2018). A survey of random forest based methods for intrusion detection systems. *ACM Computing Surveys, 51*(3), 1–36.
14. Ding, Y., & Zhai, Y. (2018). Intrusion detection system for NSL-KDD dataset using convolutional neural networks. In *Proceedings of the 2018 2nd international conference on computer science and artificial intelligence—CSAI'18*.
15. Jinarajadasa, G., Rupasinghe, L., & Murray, I. (2018). A reinforcement learning approach to enhance the trust level of MANETs. In *2018 National information technology conference (NITC)*.
16. Singh, O., Singh, J., & Singh, R. (2017). An intelligent intrusion detection and prevention system for safeguard mobile adhoc networks against malicious nodes. *Indian Journal of Science and Technology, 10*(14), 1–12.
17. Yerur, S. V., Natarajan, P., & Rangaswamy, T. R. (2017). Proactive hybrid intrusion prevention system for mobile adhoc networks. *International Journal of Intelligent Engineering and Systems, 10,* 273–283. https://doi.org/10.22266/ijies2017.1231.29.
18. Wahab, O. A., Mourad, A., Otrok, H., & Bentahar, J. (2016). CEAP: SVM-based intelligent detection model for clustered vehicular ad hoc networks. *Expert Systems with Applications, 50,* 40–54.
19. Singh, D., & Bedi, S. S. (2016). Multiclass ELM based smart trustworthy IDS for MANETs. *Arabian Journal for Science and Engineering, 41*(8), 3127–3137.
20. Kolias, C., Kambourakis, G., Stavrou, A., & Gritzalis, S. (2016). Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset. *IEEE Communications Surveys and Tutorials, 18*(1), 184–208.
21. Subba, B., Biswas, S., & Karmakar, S. (2016). Intrusion detection in mobile ad-hoc networks: Bayesian game formulation. *Engineering Science and Technology, an International Journal, 19*(2), 782–799.
22. Ahmed, M. N., Abdullah, A. H., & Kaiwartya, O. (2016). FSM-F: Finite state machine based framework for denial of service and intrusion detection in MANET. *PLoS ONE, 11*(6), e0156885.
23. Shanthi, K., Murugan, D., & Ganesh Kumar, T. (2018). Trust-based intrusion detection with secure key management integrated into MANET. *Information Security Journal: A Global Perspective, 27,* 1–9.
24. Khan, F. A., Imran, M., Abbas, H., & Durad, M. H. (2017). A detection and prevention system against collaborative attacks in mobile ad hoc networks. *Future Generation Computer Systems, 68,* 416–427.

25. Raja, R., & Ganesh Kumar, P. (2018). QoSTRP: A trusted clustering based routing protocol for mobile ad hoc networks. *Programming and Computer Software, 44*(6), 407–416.
26. Anusha, K., & Sathiyamoorthy, E. (2017). A new trust-based mechanism for detecting intrusions in MANET. *Information Security Journal: A Global Perspective, 26*(4), 153–165.
27. Luong, N. T., Vo, T. T., & Hoang, D. (2019). FAPRP: A machine learning approach to flooding attacks prevention routing protocol in mobile ad hoc networks. *Wireless Communications and Mobile Computing, 2019,* 1–17.
28. Sasirekha, D., & Radha, N. (2017). Secure and attack aware routing in mobile ad hoc networks against wormhole and sinkhole attacks. In *2017 2nd international conference on communication and electronics systems (ICCES).*
29. Ahmad, I., Basheri, M., Iqbal, M. J., & Rahim, A. (2018). Performance comparison of support vector machine, random forest, and extreme learning machine for intrusion detection. *IEEE Access, 6,* 33789–33795.
30. Yin, C., Zhu, Y., Fei, J., & He, X. (2017). A deep learning approach for intrusion detection using recurrent neural networks. *IEEE Access, 5,* 21954–21961.
31. Khan, M. A., Karim, M. R., & Kim, Y. (2019). A scalable and hybrid intrusion detection system based on the convolutional-LSTM network. *Symmetry, 11*(4), 583. https://doi.org/10.3390/sym11040583
32. Xu, C., Shen, J., Du, X., & Zhang, F. (2018). An intrusion detection system using a deep neural network with gated recurrent units. *IEEE Access, 6,* 1.
33. Elwahsh, H., Gamal, M., Salama, A. A., & El-Henawy, I. M. (2018). A novel approach for classifying MANETs attacks with a neutrosophic intelligent system based on genetic algorithm. *Security and Communication Networks, 2018,* 1–10.
34. Vimala, S., Khanaa, V., & Nalini, C. (2018). A study on supervised machine learning algorithm to improvise intrusion detection systems for mobile ad hoc networks. *Cluster Computing, 22,* 1–10.
35. Kavitha, T., Geetha, K., & Muthaiah, R. (2019). India: Intruder node detection and isolation action in mobile ad hoc networks using feature optimization and classification approach. *Journal of Medical Systems, 43*(6), 1–7.
36. Feng, F., Liu, X., Yong, B., Zhou, R., & Zhou, Q. (2018). Anomaly detection in ad-hoc networks based on deep learning model: A plug and play device. *Ad Hoc Networks, 84,* 82–89.
37. Zhang, B., Liu, Z., Jia, Y., Ren, J., & Zhao, X. (2018). Network intrusion detection method based on PCA and Bayes algorithm. *Security and Communication Networks, 2018,* 1–11.
38. Shafi, Q., Basit, A., Qaisar, S., Koay, A., & Welch, I. (2018). Fog-assisted SDN controlled framework for enduring anomaly detection in an IoT network. *IEEE Access, 6,* 1.
39. Bouhaddi, M., Radjef, M. S., & Adi, K. (2018). An efficient intrusion detection in resource-constrained mobile ad-hoc networks. *Computers and Security, 76,* 156–177.
40. Marchang, N., Datta, R., & Das, S. K. (2017). A novel approach for efficient usage of intrusion detection system in mobile ad hoc networks. *IEEE Transactions on Vehicular Technology, 66*(2), 1684–1695.
41. Zhang. (2009). Ad hoc Thesis.

M. Islabudeen received his B.E. and M.E. degree in Computer Science and Engineering from Madurai Kamaraj University and Anna University, Tamil Nadu, India in 2001 and 2008 respectively. He is currently pursuing Ph.D. in Information and Communication Engineering in Anna University, Tamil Nadu, India. He is currently working as an Associate Professor in Department of Computer Science and Engineering, Syed Ammal Engineering College, Ramanathapuram, Tamil Nadu, India. His current research interests include Cryptography and Network Security, Data Mining, Mobile Ad hoc Networks, Data Structures and Compiler Design. He is a life member of Computer Society of India (CSI) and Indian Society for Technical Education (ISTE). He has served as an active reviewer and chair of many reputed international conferences including IEEE.

Dr. M. K. Kavitha Devi received her B.E. degree in Computer Science and Engineering from Bharathidasan University, Tiruchirappalli, India in 1994 and the M.E. degree in Computer Science and Engineering from Madurai Kamaraj University, Madurai, India in 2004 and also Ph.D. degree in Information and Communication Engineering from Anna University, Chennai, India in 2011. She is currently working as a Professor in Department of Computer Science and Engineering, Thiagarajar College of Engineering, Madurai, Tamil Nadu, India. She is having more than 20 years of experience in teaching and research. Her current research interests include Recommender System, Web Intelligence, Cryptography & Information Security, Data Mining, and Data Structures. She is a member of Association of Computing Machinery (ACM) and Computer Society of India (CSI). She has more than 50 publications in reputed international conferences and refereed journals including IEEE, Springer, Elsevier, Inderscience and etc. She has served as an active reviewer, editor and chair of many international conferences and refereed journals. She is a pride recipient of the Best Computer Science Faculty Award of ASDF Global in year 2014.